12 FAM 440
POST SECURITY FUNCTIONS

(TL:DS-63; 11-26-1999)

12 FAM 441 UNASSIGNED

12 FAM 442 IDENTIFICATION CARDS

(TL:DS-39; 08-15-1994)

a. All employees, at all Foreign Service missions, annexes, and facilities having a public access control point staffed by a Marine security guard or other security personnel must show their identification card to gain access to the facility. The regional or post security officer, in coordination with the chief of mission, decides whether wearing the card while inside the facility, or within certain areas of the facility, is mandatory.

b. Post security must issue all visitors temporary identification, such as visitor sticker, identification card, badge, etc., prior to permitting access to any Foreign Service mission, annex, or facility. The visitor must wear this temporary identification in plain view at all times while in the facility. Admitting offices must escort those visitors who do not have appropriate security clearance. (See 12 FAM 445.1 for handling exceptions.)

c. Posts will establish and implement measures to safeguard identification cards, badges, passes, and other identification media. (See 12 FAM 445.2 for safeguards.)

12 FAM 443 SECURITY CLEARANCES

12 FAM 443.1 Personnel Assigned on Permanent Change of Station (PCS) Orders or Locally Hired

(TL:DS-63; 11-26-1999)

a. *Except as provided in paragraph e of 12 FAM 443.1, all U.S. citizen-U.S. Government employees either assigned through permanent change of station (PCS) or locally hired must hold a Top Secret clearance issued by their parent agency if they:*

(1) Work within a controlled access area; or

(2) Require unescorted access to a controlled access area.

The Top Secret clearance shall be based upon a Single Scope Background Investigation (SSBI) meeting the requirements of Standard B of the Investigative Standards for Background Investigations for Access to Classified Information as promulgated by the Assistant to the President for National Security Affairs or, in the case of temporary access at the Top Secret level, the Investigative Standards for Temporary Eligibility for Access.

b. All U.S. citizen-U.S. Government employees not working within a controlled access area nor requiring unescorted access to a controlled access area will possess a security clearance appropriate for the level of classified material to which they have access, and will have been the subject of an investigation appropriate for the sensitivity of the position they are occupying and the area to which they are assigned.

c. The regional security officer (RSO) or post security officer (PSO) serves as the central repository at post for clearance data.

d. It is the responsibility of the individual agencies represented at post to provide clearance data on their PCS personnel to the RSO or PSO. The options for providing this data are:

(1) The agency representative provides the data to the RSO or PSO;

(2) The agency headquarters provides the data to the RSO or PSO by official communiqué; or

(3) The agency headquarters provides the data to the Department, Bureau of Diplomatic Security, Personnel *Security*/Suitability *Division* (DS/ICI/PSS), for transmission to post.

e. For all new construction or major renovations involving controlled access areas, security clearance requirements are specified in 12 FAH-6 sections H-311.14, H-312.14, H-313.14, and H-314.14.

12 FAM 443.2 Temporary Duty Personnel

(TL:DS-63; 11-26-1999)

a. All agencies which initiate travel messages and travel authorizations for the temporary duty (TDY) assignment of their personnel (both employees and contractors) to a mission abroad, must include in the travel message and in the travel authorization the level of security clearance. In cases of TDY travel from one mission to another mission abroad, verification of security clearance level is the responsibility of the sending post.

b. Temporary duty personnel for whom clearance has not been provided to the post will not be given unescorted access to U.S. Government facilities or access to classified or controlled information.

Address requests for security clearance verification to DS/ICI/PSS with an information copy to the regional bureau and, in the case of other agency personnel, to the appropriate agency.

c. The RSO serves as the control officer for the visits of short-term (TDY) personnel on various security-related matters, e.g., emergency security support teams (see 12 FAM 444). Except in countries that are clearly on record as rejecting the accreditation of personnel assigned TDY for short periods or where attempted notification could cause other complications, the RSO will request that the chief of mission or principal officer notify the host country's foreign ministry of the impending visit of all security-related TDY visitors and request temporary accreditation for the duration of the visit.

12 FAM 444 EMERGENCY SECURITY SUPPORT

12 FAM 444.1 Policy

(TL:DS-39; 08-15-1994)

DS provides rapid operational response in emergency situations where specially trained teams of DS officers are required to supplement available overseas post or domestic office resources. Most often the team deployment will be in response to either a terrorist incident, or to an immediate threat of terrorist or criminal activity. They may also be activated for natural disasters and other unusual events.

12 FAM 444.2 Implementation

(TL:DS-39; 08-15-1994)

a. DS/DSS/OP determines the scope and work priorities of all emergency support missions. The Mobile Security Division of the Office of Professional Development (DS/PLD/MSD) is the DS office that provides support to posts for emergency situations and provides training to U.S. Government personnel and dependents at posts abroad.

b. DS/PLD/MSD will dispatch personnel and equipment quickly. To minimize the team drain on post resources, it will be as self-sufficient as possible. Posts are to arrange, to the extent possible, airport visas for team members and unimpeded entry and transportation of equipment to the mission. The team and equipment are to be en route to a post within 24 hours of a decision to deploy.

12 FAM 445 IDENTIFICATION MEDIA EXCEPTIONS AND SAFEGUARDS

12 FAM 445.1 Exception to Required Identification

(TL:DS-39; 08-15-1994)

a. There are certain areas of Department missions, annexes, and facilities where implementing this mandatory policy would inhibit operational effectiveness. USIS libraries, commercial libraries, and portions of the consular sections are examples of these areas. In these specific instances the regional or post security officer, in coordination with the chief of mission, decides which areas are exempt from this policy. This policy is primarily to enhance the post's security posture, and posts are to carefully weigh this in determining whether to make an exception for a specific area or section.

b. In the event a post determines an exception to this policy is required for a specific area or section, the post security officer will provide a full, detailed explanation to the Director for Overseas Operations (DS/OP), indicating the specific exception and the reasoning behind the exception.

12 FAM 445.2 Safeguards

(TL:DS-39; 08-15-1994)

a. Use a security container with an S&G security padlock to secure blank cards, badges, and passes. Only personnel responsible for managing the program shall have access to this container.

b. Post security must account for all cards, badges, and passes by serial number.

c. A card, badge, pass log will reflect the name, office, status (level of clearance), and expiration date for each card, badge, or pass issued. The log is a permanent part of the regional or post security office files.

d. The issuing officer will issue each card, badge, or pass issued with a written set of instructions in the proper use and safeguarding of the identification media, specifically stressing the security precautions concerning the wearing of the identification media outside of the facility.

e. Involved employees must report the circumstances surrounding lost or stolen cards, badges, or passes to the regional or post security office, which will record the circumstances.

12 FAM 446 BUILDING SECURITY ¾ LOCK AND LEAVE (L&L) POLICY

12 FAM 446.1 Policy

(TL:DS-59; 11-19-1997)

a. This policy does not advocate the elimination or removal of Marine security guards. Because of the inherent security risks for a L&L facility, the decision to implement L&L or a 24-hour cleared U.S. presence must be a risk management decision based upon vulnerabilities, asset values, threats and cost benefit analysis. This risk management process must include the participation and concurrence of the tenant agencies as well as the Department of State.

b. The L&L policy supplements 12 FAH-5, *Physical Security Handbook*, and 12 FAH-6, *OSPB Security Standards and Policy Handbook*, and addresses the minimum requirements and procedures for securing buildings (including commercial office space) that do not have 24-hour presence. Risk management may dictate technical and physical security enhancements beyond the minimum requirements.

c. L&L facilities are divided into two categories:

(1) Classified buildings where classified material is stored, discussed, or processed and without 24-hour cleared U.S. presence inside the building;

(2) Unclassified buildings where **no** classified material is stored, discussed, or processed and without 24-hour presence inside the building.

d. The L&L policy provides coverage to classified facilities from the exterior doors of a building to the outer walls of the controlled access area (CAA) on the interior of the building. The L&L policy will provide coverage to unclassified facilities based on high value assets and risk management as determined by the parent agency. (See 12 FAM 446 Exhibit 446.1 for Specific Crime Threat Requirements for Unclassified Buildings and definition of high-value assets.)

12 FAM 446.2 Facility Lock and Leave Survey

(TL:DS-59; 11-19-1997)

a. Existing classified L&L facilities will require an initial inspection by the servicing ESC/ESO. Unclassified L&L facilities with high value assets, as determined by the parent agency, will require the same inspection. A report of the inspection will be provided to DS/PSP/PSD for approval.

Existing L&L facilities with major deficiencies will require a team survey as soon as possible.

b. Prior to a new facility achieving L&L status, a team survey of the site must be performed and survey recommendations implemented.

c. The survey team will be composed of at least one member of DS/PSP/PSD and at least one member from the servicing ESC/ESO, and the tenant agency if applicable. The team will work in close cooperation with post management and the RSO/PSO.

d. The survey team must review all existing pertinent post information (e.g., reports, surveys, exceptions, etc.) prior to departure for post.

e. The survey team will include in a survey report, at a minimum, the following items:

(1) A compilation of existing post information;

(2) Site information which is pertinent to the decision process; (e.g., location of local police stations, neighboring dwellings, past history of incidents, political significance of site, building setback, perimeter structures, existing security measures, etc.);

(3) A detailed description of the building's structural limitations and composition, with emphasis on exterior walls, doors, and windows;

(4) Floor layout drawings, including areas of special interest (e.g., proposed L&L and bypass door locations, public access control (PAC) location, systems interface cabinet (SIC) room, CAA location(s), proposed technical equipment layout, description of typical personnel traffic flow, applicable high value item locations, etc.);

(5) A general overview of the level, volume, and significance of classified material stored at post, if applicable;

(6) A list of physical and technical security items required to bring the building into compliance with the L&L policy;

(7) A full description of both the proposed L&L door and the bypass door (i.e., type, existing hardware, swing, etc.) as defined in 12 FAM 446.3;

(8) Locations of key areas in the building for possible time-lapse CCTV coverage (e.g., areas contiguous to CAA, hallway intersection points, stairwells, etc.);

(9) Identify post specific alarm response options (e.g., post personnel, guards, police, 24-hour remote monitoring, etc.);

(10) A general view of how post management envisions the L&L operation to function for a particular building.

f. A copy of the L&L site survey report will be retained by the servicing ESC/ESO and post security officer. DS/PSP/PSD will provide additional copies to all concerned parties.

12 FAM 446.3 General Requirements

12 FAM 446.3-1 Physical Security

(TL:DS-59; 11-19-1997)

a. Each L&L facility will have only one door, designated the L&L door, for use after office hours. This door will be the last point of exit/initial point of entry of a L&L building. Locking hardware for this door is identified in 12 FAH-5, *Physical Security Handbook*, as SHW-18 (opaque door) or SHW-18A (transparent door).

b. All exterior forced entry (FE) doors must have the door manufacturer's threshold plate installed and be in accordance with the manufacturer's specifications.

c. In the eventuality of an electrical or mechanical lockout of the L&L door, a separate door equipped with bypass hardware will be provided when possible. See 12 FAM 446.4 and 12 FAM 446.5 for bypass door hardware requirements for each particular facility type.

12 FAM 446.3-2 Technical Security

(TL:DS-59; 11-19-1997)

a. All classified facilities and any unclassified facility with high-value assets will require the installation of a separate DS-approved alarm system dedicated to L&L for the purpose of monitoring designated alarm points:

(1) The alarm system must have a system status indicator;

(2) The alarm system must be activated and deactivated via a personal identification number (PIN) or other DS-approved device, located on the interior wall adjacent to the designated L&L door. The PIN pad must be positioned to preclude visual compromise from the building exterior;

(3) The assignment of PIN pad numbers must be random in nature and consist of five or more digits/characters;

(4) The alarm system PIN pad status indicator or other DS-approved device will reflect system violations and must be cleared with a unique user acknowledgment;

(5) The alarm system must have date and time stamping which can be used to determine when and for how long an intrusion occurred;

(6) All alarm devices will be individually zoned or configured as separate identifiable alarm points;

(7) All building exterior doors must be monitored by the L&L alarm system;

(8) The alarm system panel and the L&L door access system panel must be located in the SIC room. If there is not an existing SIC room, one of appropriate size must be established to house the equipment. The room must provide the necessary electrical service, ventilation, and floor to ceiling construction;

(9) The SIC room door must be equipped with a DS-approved deadbolt lock and monitored by the L&L alarm system. In addition to the standard hardware, a GSA-approved dial combination lock is recommended for the SIC room door at high and critical technical threat posts. See SHW-17 door hardware group identified in 12 FAH-5, *Physical Security Handbook*;

(10) Power for the L&L time-lapse video and alarm system equipment must be regulated and supported by battery backup or UPS system;

(11) A dedicated power supply with a backup battery of at least 6.5 AH must be provided for the L&L door when utilizing SHW-18 or SHW-18A hardware;

(12) For posts with classified facilities, the L&L alarm and door access system panel(s) must be tamper alarmed whenever possible;

(13) All volumetric detectors of the L&L alarm system must be tamper alarmed.

b. If time-lapse video hardware and recording equipment is required, it must be DS-approved equipment. See 12 FAM 446 Exhibit 446.3-2 for Specific Technical Threat Requirements (for the utilization of time-lapse video).

c. The time-lapse video system must be housed in a locked DS-approved container located in the CAA.

12 FAM 446.3-3 Operational Security

(TL:DS-59; 11-19-1997)

a. The RSO/PSO will establish appropriate post specific methods and procedures for informing the duty officer and other designated person(s) of any L&L alarm activation.

b. After each L&L alarm activation, a designated cleared U.S. citizen will log the time and date of the event, review any applicable recording media results and investigate the cause of the anomaly. Unexplained findings will be immediately reported to the RSO for appropriate action.

c. The following procedures for exiting the L&L facility apply:

(1) All exterior doors (with the exception of the L&L door) will be internally secured in one of the following manners:

(a) The forced entry locks (or equivalent DS-approved locking system) will be engaged;

(b) Facilities with non-FE exterior doors, will be secured with a DS-approved 1-inch deadbolt or equivalent locking device;

(2) Entries into a L&L log book (or equivalent DS-approved methodology) must be made upon initial lockup or opening, and upon any after-hours entry or departure;

(3) The L&L alarm system must be activated via a PIN pad or other DS-approved device prior to exiting the building;

(4) The L&L door will be secured by the appropriate locking devices as outlined in the SHW-18 or SHW-18A hardware groups.

d. Security officer duties and responsibilities:

(1) The RSO/PSO, in conjunction with the emergency action committee, will establish procedural guidelines for L&L alarm response;

(2) The RSO/PSO will control and maintain the L&L door combination (if applicable) and the alarm system/door access system PIN pad numbers in accordance with 12 FAM 532.2-1 and 12 FAM 532.2-2.

e. All malfunctions and anomalies of the L&L system must be reported immediately to the cognizant RSO and servicing ESC/ESO. Affected tenant agency headquarters will be notified through DS.

12 FAM 446.4 Classified L&L Buildings

(TL:DS-59; 11-19-1997)

a. The L&L policy for classified buildings, as defined in 12 FAM 446, is primarily designed for technical threat. See 12 FAM 446 Exhibit 446.3-2 and 12 FAM 446 Exhibit 446.4 (Specific Crime Threat Requirements for Classified Buildings) for threat specific requirements.

b. All L&L system new wiring must be in ferrous conduit with compression fittings.

c. The installation and final hook-up of the L&L system must be performed by an SEO, Seabee, or other qualified cleared U.S. citizen.

d. The completed installation will be inspected and approved by DS.

e. Post management and security professionals (RSO/SEO) must develop a standard operating procedure (SOP) plan for securing the building in accordance with this directive. Assistance in the preparation of this plan may be provided by DS/PSD/PCB upon request.

f. If authorized by the RSO/PSO, Foreign National employees and local guards may continue to work within their general work areas, providing a cleared U.S. citizen is in the building and the lock down sweep has not yet occurred. The cleared U.S. citizen must be cognizant of all personnel working after normal office hours.

g. At a post established time, a designated cleared U.S. citizen(s) will be responsible for locking down the building after ensuring that it is void of all personnel.

h. A designated cleared U.S. citizen(s) will be responsible for re-opening the building.

i. An after-hours sign in/out log book (or equivalent DS-approved method) must be provided adjacent to the L&L alarm system's activation/deactivation device to minimize life-safety and fire issues.

j. All after-hours entries (i.e., after the L&L building has been locked down) must be verified the next working day by the PSO or duty officer.

k. The DS-approved alarm system must be hardwired at facilities, which store, discuss, or process material classified above Confidential.

l. The DS-approved L&L alarm system should have two methods of reviewing a triggered alarm event (e.g., real-time printer, alarm panel down-loadable event memory, etc.).

m. The volumetric detection devices should be augmented (depending on threat level) with alarm activated video coverage and time-lapse video recording at key locations as determined from the site survey. See 12 FAM 446 Exhibit 446.3-2 for threat-specific requirements.

n. L&L bypass door hardware is determined by threat level. See 12 FAM 446 Exhibit 446.3-2 for threat-specific requirements.

o. The L&L bypass door must be protected on the interior side with a volumetric detection device.

p. Removable lock cores on all exterior doors and the SIC room door must be changed every year at high and critical technical threat posts, and

every two years at low and medium technical threat posts. In the event of a suspected compromise of the building, the responding SEO or other qualified cleared U.S. citizen must exchange the cores, including spares, with cores brought securely from off-site locations. The replacement cores must not be shipped ahead of time and stored at post. However, as an interim measure the cores must be changed immediately using on-site spares.

q. Spare L&L removable lock cores and their keys must be stored in a Class 5 container under the direct control of the resident RSO/PSO. The Class 5 container will be fitted with the latest GSA-approved dial combination lock.

r. A test of the L&L technical security system must be performed on a quarterly basis and after the occurrence of a suspected compromise. The inspection should include all exterior door locking systems, a hostile walk test of the alarm system (i.e., to include all applicable doors, time stamped video [if applicable], and volumetric detection devices), and all duty officer alerting equipment. (Hostile walk test: probing of volumetric detection capabilities through floor crawl methods, slipping along walls, vertical walk probing, etc.) Testing must be performed by an SEO or other technically qualified cleared U.S. citizen.

s. The following key control procedures will apply:

(1) The exterior removable cores of the forced entry locks on the L&L bypass door must be keyed differently with no master or grandmaster key;

(2) The facility bypass door key(s) are to reside in a locked and tamper alarmed DS-approved depository container located external to the building. It must be anchored or imbedded securely to the building structure;

(3) The technical equipment room must be keyed differently with no master or grandmaster key;

(4) Keys to the L&L technical equipment room must be tracked during work hours and secured at the end of each work day by the PSO or duty officer.

12 FAM 446.5 Unclassified L&L Buildings

(TL:DS-59; 11-19-1997)

a. The L&L policy for unclassified buildings, as defined in 12 FAM 446, is primarily designed for criminal threat. See 12 FAM 446 Exhibit 446.1 for threat-specific requirements.

b. The DS-approved alarm system may be hard-wired or wireless. If a wireless system is selected, it must utilize spread spectrum or comparable technology and have a hardwired keypad.

c. Wiring for the L&L system can be in ferrous or PVC conduit, panduit, or equivalent.

d. Post management and security professionals (RSO/SEO) must develop an SOP for building lock-down.

e. The designee responsible for lock down must ensure that the building is void of all personnel.

f. An after-hours sign in/out log book (or equivalent DS-approved methodology) is required to minimize fire and life-safety issues.

g. A test of the L&L technical security system must be performed on a biannual basis and after the occurrence of any suspected compromise. Inspection should include all exterior door-locking systems, walk test of alarm system (i.e., to include all applicable doors, volumetric detection devices, and duty officer alerting equipment). The test must be performed by technically competent authorized personnel.

h. The L&L bypass door must have one of the following options:

(1) A DS-approved 1-inch deadbolt lock with external keyway;

(2) An existing SHW-8 emergency exit door retrofitted with an external pull handle and keyway. This allows key access by retracting the latch of the panic exit device via the external keyway while activating the time delay module. After the expiration of the time delay the door can be opened via the pull handle.

i. Removable lock cores of all exterior doors must be changed after any suspected comprise of the building.

j. The following key control procedures will apply:

(1) The L&L bypass door and technical equipment room must be keyed differently with no master or grandmaster key;

(2) The facility bypass door keys are the responsibility of the RSO/PSO;

(3) Keys to the L&L technical equipment room are the responsibility of the RSO/PSO.

12 FAM 447 THROUGH 449 UNASSIGNED

12 FAM 446 Exhibit 446.1
SPECIFIC CRIME THREAT REQUIREMENTS FOR UNCLASSIFIED BUILDINGS

(TL:DS-59; 11-19-1997)

Unclassified Buildings	Crime Threat			
	Critical	High	Medium	Low
The L&L alarm system requires monitoring devices on all exterior doors and the room housing the alarm equipment.	Yes	Yes	Yes	Yes
Interior building doors of offices containing high value assets* will be monitored. Doors must be fitted with automatic closers.	Yes	Yes	Yes	Yes
Volumetric protection for office areas containing high value assets.*	Yes	Yes	No[1]	No

KEY

1 - Facilities with exterior walls, windows and doors (as applicable), below 16' above grade or accessible platforms, that do not meet forced entry (FE) standards for the particular facility type as outlined in 12 FAH-5 require volumetric protection for office areas containing high value assets.

*** High Value Assets** - Items whose compromise or loss will severely impact post operations (e.g., PC system containing personnel or payroll data, safes containing funds, etc.).

12 FAM 446 Exhibit 446.3-2
SPECIFIC TECHNICAL THREAT REQUIREMENTS

(TL:DS-59; 11-19-1997)

Classified Buildings	Technical Threat			
	Critical	High	Medium	Low
The L&L bypass door requires external keyway forced entry locks.	Yes	Yes	Yes	Yes
If an SHW-8 door is used as the L&L bypass door, it requires retrofitting with a pull handle and external keyway. The key retracts the panic exit device latch and activates the time-delay. After the time delay expires, the door can be opened via the pull handle.	Yes	Yes	Yes	Yes
Volumetric protection of key points as determined from the site survey.	Yes	Yes	Yes	No
Volumetric detection devices will be augmented with alarm activated video coverage and time-lapse video recording at key locations determined from the site survey.	Yes	Yes	No[2]	No
Exterior time-lapse video coverage of the L&L door and bypass key container must be provided for after-hours entries and L&L alarm events.	Yes	Yes	No[2]	No
Interior time-lapse video coverage of the bypass door area must be provided for L&L alarm events.	Yes	Yes	No[2]	No
A wireless intrusion alarm system with spread spectrum or comparable masking protection communication techniques may be utilized.	No	Yes[1]	Yes[1]	Yes[1]

KEY

1 - Facilities, which store, discuss, or process classified material above the level of Confidential must use a hardwired alarm system.

2 - Video coverage may be extended to medium technical threat posts, which are rated high for human intelligence threat. This is to be evaluated by DS/CIS/IST upon recommendation by CIWG.

12 FAM 446 Exhibit 446.4
SPECIFIC CRIME THREAT REQUIREMENTS FOR CLASSIFIED BUILDINGS

(TL:DS-59; 11-19-1997)

Classified Buildings	Crime Threat			
	Critical	High	Medium	Low
Interior building doors of offices containing high value assets* will be monitored. Doors must be fitted with automatic closers.	Yes	Yes	Yes	Yes
Volumetric protection for office areas containing high value assets.*	Yes	Yes	No	No

*** HIGH VALUE ASSETS -** Items whose compromise or loss will severely impact post operations (e.g., PC system containing personnel or payroll data, safes containing funds, etc.).